Wydatek współfinansowany z Europejskiego Funduszu Społecznego

Opis Przedmiotu Zamówienia

A. PRZEDMIOT UMOWY

1. W ramach niniejszej Umowy Wykonawca zobowiązuje się zapewnić Zamawiającemu wsparcie na utrzymanie i monitorowanie sieci oraz korelowanie zdarzeń bezpieczeństwa Obszarach Technologicznych na zasadach określonych Umowie oraz w załącznikach do niej, które to wsparcie przede wszystkim zapewnić ma poprawne i nieprzerwane działanie każdego z Obszarów Technologicznych.
2. Wsparcie na utrzymanie sieci obowiązuje przez 12 miesięcy.
3. W ramach usługi wsparcia Wykonawca zapewni poprawne i nieprzerwane działanie poszczególnych Obszarów Technologicznych poprzez:
    1) usuwanie Błędów - zgodnie z załącznikiem nr 1 do Umowy „Gwarantowany poziom naprawiania błędów (SLA)";
    2) udzielanie pracownikom Zamawiającego konsultacji, porad i zaleceń, dokonywanie Proaktywnych Przeglądów Okresowych, konfigurowanie oprogramowania, wdrażanie poprawek i aktualizacji oprogramowania, podniesienie wersji oprogramowania, wykonywanie własnych kopii bezpieczeństwa i przywracanie Obszarów Technologicznych - zgodnie z załącznikiem 2 do Umowy „Gwarantowany poziom świadczenia usług dodatkowych (SLA)";
4. Poszczególne Obszary Technologiczne podlegające wsparciu posiadane przez Zamawiającego to:
    1) Routery Brzegowe - Cisco,
    2) Przełączniki LAN – Brocade ICX,
    3) Urządzenia bezpieczeństwa – Palo Alto Networks,
    4) Urządzenia sieci bezprzewodowej WiFi/WLAN,
    5) System OpenSource wspomagający zarządzanie siecią – Zabbix,
    6) Systemy OpenSource monitorowania i korelacji zdarzeń bezpieczeństwa rozwiązania SIEM - ELK Stack,
    7) System OpenSource skanowania podatności - Greenbone.
5. Zamawiający dopuszcza świadczenie usług przewidzianych niniejszą Umową poprzez zdalny dostęp tylko wtedy, gdy łącznie zostaną spełnione następujące warunki:
    - zasady zdalnego dostępu zostały szczegółowo uregulowane w załączniku do Umowy;
    - dla danej usługi wyraźnie przewidziano w Umowie lub załączniku do niej możliwość jej świadczenia z wykorzystaniem zdalnego dostępu.

6. Wykonawca zobowiązuje się wykonywać przedmiot Umowy z należytą starannością wymaganą przy usługach tego rodzaju przy zachowaniu zasad współczesnej wiedzy i zgodnie z obowiązującymi w tym zakresie przepisami, zgodnie z najlepsza praktyką i wiedzą zawodową, uwzględniając profesjonalny charakter swojej działalności, w sposób i w terminach określonych w Umowie oraz w załącznikach do niej stanowiących jej integralną część.
7. Wykonawca zapewnia, że dysponuje odpowiednim potencjałem techniczno-organizacyjnym, jak również wiedzą i doświadczeniem, pozwalającymi należycie wykonywać przedmiot Umowy.
8. Wykonawca gwarantuje, że posiada personel o kwalifikacjach zawodowych, doświadczeniu i wykształceniu niezbędnym do wykonywania przedmiotu Umowy zgodnie z wymaganiami opisanymi w Ogłoszeniu o zamówieniu oraz w Umowie i załącznikach do niej.
9. Wszystkie wymienione urządzenia i systemy są w posiadaniu i w użyciu przez Zamawiającego.
10. Zakup jakichkolwiek urządzeń, czy systemów nie jest przedmiotem postępowania

B. OBOWIĄZKI WYKONAWCY I PARAMETRY SLA

1. Wykonawca odpowiada za poprawne i nieprzerwane działanie Obszarów Technologicznych zgodnie z parametrami SLA zdefiniowanymi w niniejszym dokumencie i związku z tym zobowiązany jest on do usuwania Błędów w Czasie Naprawy. Celem usunięcia wątpliwości Strony zgodnie oświadczają, że usunięcie Błędu może również polegać na konfiguracji oprogramowania wchodzącego w skład Obszarów Technologicznych.
2. Dla uniknięcia wątpliwości przyjmuje się, że Wykonawca usunie wszelkie zgłoszone przez Zamawiającego Błędy, w tym także po zakończeniu okresu świadczenia usługi (także na skutek odstąpienia od Umowy Głównej lub jej wypowiedzenia), o ile zostaną one zgłoszone przed upływem tego okresu.
3. Zamawiający dopuszcza wykonywanie obowiązków przewidzianych w niniejszym dokumencie przez Personel Wykonawcy.
4. Zamawiający dopuszcza wykonywanie obowiązków przewidzianych w niniejszym dokumencie z wykorzystaniem zdalnego dostępu.
5. Wykonawca gwarantuje następujące Czasy Reakcji:

Błąd Krytyczny	Czas Reakcji zgodnie z ofertą Wykonawcy, nie dłuższy niż 4 godziny zegarowe.
Błąd niekrytyczny	Czas Reakcji wskazany w ofercie Wykonawcy, nie dłuższy niż 8 godzin roboczych
Usterka	Czas Reakcji wskazany w ofercie Wykonawcy, nie

	dłuższy niż 12 godziny robocze

6. Wykonawca gwarantuje Zamawiającemu następujące Czasy Naprawy:

Błąd Krytyczny	Czas Naprawy zgodnie z ofertą Wykonawcy, nie dłuższy niż 8 godziny zegarowe.
Błąd niekrytyczny	Czas Naprawy określony w ofercie Wykonawcy, nie dłuższy niż 16 godzin roboczych
Usterka	Czas Naprawy określony w ofercie Wykonawcy, nie dłuższy niż 24 godziny robocze

7. Wykonawca gwarantuje Zamawiającemu następujące czasy analizy danych agregowanych w Systemach wymienionych w § 1 pkt 4, ppkt 7 i 8 Umowy Głównej i informowania o zdarzeniach (alertach) i informacjach poprzez przesłanie wiadomości na wskazane przez Zamawiającego adresy email, w całym okresie trwania umowy:

Priorytet Krytyczny	Czas reakcji i informowania o problemie nie dłuższy niż 4 godziny robocze.
Priorytet Wysoki	Czas reakcji i informowania o problemie nie dłuższy niż 4 godziny robocze.
Priorytet niski	Czas reakcji i informowania o problemie nie dłuższy niż 12 godzin roboczych.

8. Godzina zegarowa to każde kolejne 60 minut od poniedziałku do niedzieli.
9. Godzina robocza to każde kolejne 60 minut w przedziale czasowym od 8:00 do 16:00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

10. Jeżeli Czas Naprawy będzie się kończyć poza godzinami roboczymi u Zamawiającego, automatycznie ulega on przedłużeniu do następnego dnia roboczego u Zamawiającego.[1]
11. Zamawiający oświadcza, że posiada stosowne licencje, które zezwalają m.in. na trwałe lub czasowe zwielokrotnianie programów komputerowych zawierających się w poszczególnych Obszarach Technologicznych oraz na dokonywanie tłumaczenia, przystosowania, zmiany układu lub dokonywania jakichkolwiek innych zmian w powyższych programach komputerowych, jeżeli jest to niezbędne do poprawiania występujących w nich błędów.
12. Wykonawca zobowiązuje się do usuwania Błędów z należytą starannością wymaganą przy usługach tego rodzaju przy zachowaniu zasad współczesnej wiedzy i zgodnie z obowiązującymi w tym zakresie przepisami, zgodnie z najlepsza praktyką i wiedzą zawodową, uwzględniając profesjonalny charakter swojej działalności, w sposób i w terminach określonych w niniejszym dokumencie. Nadto, Wykonawca zapewnia, że:
    - dysponuje odpowiednim potencjałem techniczno-organizacyjnym oraz osobowym, jak również wiedzą i doświadczeniem pozwalającym należycie usuwać Błędy;
    - usuwając Błędy osobiście lub przez podmioty z nim powiązane nie naruszy przepisów prawa, jak również praw podmiotów trzecich, w szczególności przysługujących podmiotom trzecim praw autorskich, praw z rejestracji wzorów przemysłowych, praw ochronnych na znaki towarowe oraz dóbr osobistych.

C. ZGŁOSZENIE BŁĘDU I NAPRAWA

1. W przypadku wykrycia przez Zamawiającego Błędu dokona on jego zgłoszenia oraz nada mu status (Błąd Krytyczny/Błąd Niekrytyczny/Usterka). Wskazany przez Zamawiającego status Błędu jest wiążący dla Wykonawcy.
2. Zamawiający ma prawo zmienić status Błędu na niższy, w szczególności po otrzymaniu od Wykonawcy informacji, o której mowa ustępie 10 lit. a Sekcji C w Załączniku nr 1 Do Umowy.
3. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje nt. nieprawidłowego działania danego Obszaru Technologicznego istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości w działaniu tego Obszaru Technologicznego. System zgłoszeniowy udostępniony przez Wykonawcę nie może uzależniać rozpoczęcia obsługi zgłoszenia od przekazania innych informacji niż opis Błędu i znane Zamawiającemu okoliczności jego wystąpienia ani nie może wymagać określonego stopnia szczegółowości tych opisów.
4. Wykonawca zobowiązuje się rejestrować zgłaszane Błędy wykorzystując rozwiązania techniczne oraz informatyczne umożliwiające raportowanie zgłoszeń wraz z danymi pozwalającymi m.in. na śledzenie czasu ich usunięcia, a w szczególności Czasu Reakcji oraz Czasu Naprawy za pomocą aplikacji serwisowej (systemu zgłoszeniowego) udostępnionej przez Wykonawcę, W razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Błędu z innego źródła niż zgłoszenie Zamawiającego, Wykonawca zobowiązany jest do

[1] Na przykład: jeżeli Zamawiający zgłosi Błąd Krytyczny o godzinie 14:00 w poniedziałek, naprawa błędu powinna zakończyć się najpóźniej do godziny 8:00 dnia następnego.

podjęcia stosownych działań przewidzianych dla Czasu Reakcji oraz niezwłocznego poinformowania Zamawiającego o wystąpieniu Błędu.

5. Wykonawca zapewnia, że zgłoszenia Błędów mogą być dokonywane zgodnie z ofertą Wykonawcy, która stanowi załącznik do Umowy Głównej, jednakże co najmniej od poniedziałku do piątku w godzinach od 8 do 16 z wyłączeniem dni ustawowo wolnych od pracy.
6. Wykonawca zobowiązany jest do potwierdzenia przyjęcia zgłoszenia odpowiednim wpisem w aplikacji serwisowej.
7. W Czasie Reakcji Wykonawca zobowiązany jest ustalić przyczynę (diagnoza), która spowodowała Błąd, a następnie zgłosić Zamawiającemu przystąpienie do naprawy Błędu. Najpóźniej w chwili zgłoszenia przystąpienia do naprawy Błędu powinien przekazać Zamawiającemu następujące informacje:
    a) jaki status w ocenie Wykonawcy ma zgłoszony Błąd (Błąd Krytyczny, Błąd Niekrytyczny, Usterka);
    b) jaka jest przyczyna Błędu;
    c) ile w jego ocenie potrwa w przybliżeniu naprawa Błędu.
8. Czas Naprawy uważa się za dochowany z chwilą zgłoszenia Zamawiającemu dokonania naprawy, pod warunkiem, że Błąd oraz jego przyczyna zostały całkowicie i skutecznie usunięte wskutek czego została przywrócona pełna funkcjonalność danego Obszaru Technologicznego istniejąca przed wystąpieniem Błędu. Jeżeli podczas weryfikacji usunięcia Błędu okaże się, że Błąd nie został usunięty, Czas Naprawy jest dochowany dopiero z chwilą zgłoszenia poprawki faktycznie usuwającej Błąd. W celu usunięcia wątpliwości Strony zgodnie oświadczają, że jeżeli po dokonaniu naprawy Błędu poszczególne Obszary Technologiczne nie będą ze sobą współpracować w taki sposób, w jaki współpracowały przed wystąpieniem Błędu, naprawa nie jest dokonana.
9. Wraz z informacją o usunięciu Błędu Wykonawca prześle Zamawiającemu informację o przyczynie Błędu wraz ze zwięzłym opisem czynności jakie zostały podjęte w celu jego naprawienia.
10. Zamawiający ma obowiązek dokonać weryfikacji usunięcia Błędu w terminie 4 godzin roboczych licząc od chwili zgłoszenia przez Wykonawcę dokonania naprawy. Celem usunięcia wątpliwości Strony oświadczają, że niedochowanie wyżej wymienionego terminu nie oznacza przyznania przez Zamawiającego, że Błąd został naprawiony.

D. KONSULTACJE

1. W ramach obowiązku udzielania pracownikom Zamawiającego konsultacji dotyczących infrastruktury informatycznej (całokształt rozwiązań sprzętowo-programowych) związanej z Obszarami Technologicznymi Wykonawca zapewni konsultantów, którzy będą posiadać odpowiednią wiedzę i doświadczenie w zakresie oprogramowania, w tym jego konfiguracji wchodzącego w skład Obszarów Technologicznych.
2. Istotą konsultacji jest to, aby pracownicy Zamawiającego w możliwie jak najkrótszym czasie otrzymywali odpowiedzi, które mają prowadzić do rozwiązania konkretnych problemów związanych z infrastrukturą informatyczną.
3. Zamawiający dopuszcza możliwość udzielania konsultacji przez podwykonawców. Wykonawca zapewnia, że w takim przypadku podwykonawca będzie zobowiązany do świadczenia usługi konsultacji na dokładnie

takich samych warunkach, na jakich zobowiązany jest sam to robić. Wykonawca odpowiada za jakość udzielonych przez podwykonawcę konsultacji.

4. Konsultacje będą świadczone co najmniej telefonicznie (np. centrum obsługi telefonicznej, biuro obsługi klienta) oraz z wykorzystaniem poczty elektronicznej i komunikatora Skype, a jeżeli Wykonawca przewiduje także inne sposoby komunikacji, np. chat, sms, wszelkiego rodzaju komunikatory, także z wykorzystaniem tych sposobów komunikacji.
5. Najpóźniej do godziny 9:00 dnia następnego po wejściu w życie Umowy Głównej Wykonawca przekaże Zamawiającemu wszelkie informacje niezbędne do korzystania z konsultacji w sposób podany w ustępach poprzednich, a w szczególności przekaże Zamawiającemu numer telefonu, adres e-mail oraz identyfikator Skype.
6. Wykonawca zapewnia, że Zamawiający będzie mógł korzystać z konsultacji od poniedziałku do piątku w godzinach od 8:00 do 16:00 z wyłączeniem dni ustawowo wolnych od pracy.
7. Do korzystania z konsultacji uprawnieni są wyłącznie pracownicy Zamawiającego.
8. Konsultant ma prawo dokonać weryfikacji czy zgłaszający się po konsultacje jest do tego uprawniony, o ile Wykonawca wcześniej określi stosowną procedurę weryfikacji i przekaże jej szczegóły Zamawiającemu.
9. W przypadku konsultacji prowadzonych telefonicznie lub przy pomocy komunikatora Skype pracownik Zamawiającego ma prawo zażądać od konsultanta potwierdzenia zaproponowanego mu rozwiązania problemu. Wówczas treść informacji stanowiącej odpowiedź Wykonawca niezwłocznie prześle na co najmniej jeden z adresów e-mail podanych w Umowie Głównej do kontaktu z Zamawiającym, wskazany mu przez pracownika Zamawiającego.
10. Jeżeli pracownik Zamawiającego uzna, że:
    a) konsultant nie udzielił odpowiedzi na zadane mu pytanie albo
    b) udzielona przez konsultanta odpowiedź nie wyczerpuje jego wątpliwości albo
    c) konsultant stwierdzi, że nie jest w stanie odpowiedzieć na zadane pytanie albo
    d) istnieje stosowna potrzeba,

    – ma prawo zwrócić się do Wykonawcy z pytaniem zadanym na piśmie lub z wykorzystaniem poczty elektronicznej (adresy do kontaktu z Wykonawcą podane są w Umowie Głównej). Wykonawca zapewnia zaś, że zatrudnia osoby, które posiadają wykształcenie, wiedzę i doświadczenie, które umożliwią udzielenie pytającemu wyczerpującej odpowiedzi.
11. Wykonawca zobowiązuje się, że udzieli odpowiedzi na zadane przez pracownika Zamawiającego na piśmie lub przy pomocy poczty elektronicznej pytanie najpóźniej w ciągu 16 godzin roboczych[2] licząc od chwili przekazania pytania. Odpowiedź powinna być udzielona co najmniej z wykorzystaniem poczty elektronicznej jednocześnie na wszystkie podane w Umowie Głównej do kontaktu z Zamawiającym adresy e-mail.
12. W szczególnie uzasadnionych przypadkach Zamawiający - w odpowiedzi na należycie umotywowaną prośbę Wykonawcy - może odpowiednio wydłużyć termin do udzielenia odpowiedzi. Uzasadnionym przypadkiem

[2] Godzina robocza to każde kolejne 60 minut w przedziale czasowym od 8:00 do 16:00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Za pierwszą minutę godziny roboczej należy uznać tę, w której nastąpiło określone zdarzenie.

może być np. potrzeba zapoznania się przez Wykonawcę ze środkami technicznymi znajdującymi się w siedzibie Zamawiającego. Wydłużenie powyższego terminu nie może być potwierdzone ustnie (np. telefonicznie).

E. DORADZTWO

1. Zamawiający przewiduje tworzenie nowej infrastruktury informatycznej oraz nowych usług informatycznych i w związku z tym oczekuje także od Wykonawcy doradztwa w powyższym zakresie. Wykonawca zobowiązuje się świadczyć na rzecz Zamawiającego takie doradztwo, a w szczególności w zakresie następujących tematów:
    1) optymalizacja infrastruktury informatycznej (całokształt rozwiązań sprzętowo-programowych), a w szczególności związanej z Obszarami Technologicznymi (np. wskazanie o ile niezbędne jest zwiększenie zasobów przypisanych do poszczególnych Obszarów Technologicznych po to, aby zapewniały one poprawną pracę tych obszarów);
    2) rozbudowa infrastruktury informatycznej (np. wskazanie potrzeby rozbudowy infrastruktury informatycznej lub wymiany sprzętu),
    3) reinstalacja oprogramowania,
    4) kolejne przedsięwzięcia informatyczne.

F. PROAKTYWNE PRZEGLĄDY OKRESOWE

W ramach obowiązku przeprowadzania Proaktywnych Przeglądów Okresowych Wykonawca zobowiązuje się na żądanie Zamawiającego do przeprowadzania weryfikacji poprawności funkcjonowania poszczególnych Obszarów Technologicznych. PPO w szczególności polegać będzie na analizie podstawowych logów w odniesieniu do poszczególnych Obszarów Technologicznych oraz poziomu ich aktualizacji.

G. POMOC TECHNICZNA

W ramach pomocy technicznej Wykonawca zobowiązany będzie do wykonania:

1) prac związanych z konfiguracją oprogramowania wchodzącego w skład Obszarów Technologicznych;
2) prac polegających na aktualizowaniu oprogramowania wchodzącego w skład Obszarów Technologicznych;
3) prac polegających na podnoszeniu wersji oprogramowania wchodzącego w skład Obszarów Technologicznych do najnowszych wersji;
4) wykonywania kopii bezpieczeństwa oraz przywracania Obszarów Technologicznych z wykonanych przez siebie kopii bezpieczeństwa.

1. W ramach wsparcia na utrzymanie sieci Wykonawca zobowiązany jest na żądanie Zamawiającego wdrożyć poprawki lub aktualizacje do oprogramowania wchodzącego w skład Obszarów Technologicznych.
2. W terminie 24 godzin roboczych - licząc od chwili otrzymania żądania wystosowanego przez Zamawiającego - Wykonawca dokona oceny czy żądana poprawka lub aktualizacja w jego ocenie powinna być czy też nie powinna być wdrożona, i przedstawi Zamawiającemu zwięzłe uzasadnienie swojego stanowiska.

3. Wykonawca może przystąpić do prac związanych z wdrożeniem poprawki lub aktualizacji dopiero po uzyskaniu akceptacji Zamawiającego.
4. Poprawka lub aktualizacja powinna zostać wdrożona w czasie 24 godzin roboczych licząc od chwili otrzymania akceptacji Zamawiającego, a w przypadku, w którym Zamawiający zwolni Wykonawcę od obowiązku wykonania oceny, o której mowa w ust. 2, w terminie 24 godzin roboczych licząc od chwili otrzymania informacji o zwolnieniu Wykonawcy z tegoż obowiązku.
5. Wykonawca zobowiązany jest poinformować Zamawiającego o zakończeniu prac związanych z wdrożeniem poprawki lub aktualizacji.
6. Prace związane z wdrożeniem poprawek i aktualizacji nie mogą być wykonywane w godzinach roboczych u Zamawiającego jeżeli mogłoby to doprowadzić do sytuacji, w której nie byłoby możliwe korzystanie z danego Obszaru Technologicznego zgodnie z jego przeznaczeniem.
7. Zamawiający dopuszcza możliwość wykonywania prac związanych z aktualizacją oprogramowania przy pomocy zdalnego dostępu.
8. Zamawiający zapewnia, że posiada stosowne licencje udzielone przez producentów oprogramowania, które umożliwiają wykonywanie czynności aktualizacyjnych przewidzianych w niniejszym paragrafie.
9. Wykonawcy należeć się będzie wynagrodzenie wyłącznie za prace związane z aktualizacją oprogramowania lub wdrożeniem poprawek na zasadach określonych w niniejszym dokumencie oraz w Umowie Głównej. Pozostałe czynności przewidziane w niniejszym paragrafie Wykonawca wykona nieodpłatnie.

H. PODNOSZENIE WERSJI OPROGRAMOWANIA

1. W ramach pomocy technicznej Wykonawca zobowiązany jest także dokonać na żądanie Zamawiającego podniesienia wersji następujących Obszarów Technologicznych:
    1) Aktualizacja oprogramowania na urządzeniach LAN
    2) Aktualizacja oprogramowania na routerach Cisco
    3) Aktualizacja oprogramowania na urządzeniach bezpieczeństwa Palo Alto
    4) Aktualizacja oprogramowania na urządzeniach sieci bezprzewodowej WiFi/WLAN
    5) Aktualizacja oprogramowania OpenSource wspomagające zarządzanie siecią – Zabbix
    6) Aktualizacja oprogramowania OpenSource monitorowania i korelacji zdarzeń bezpieczeństwa SIEM - ELK stack
    7) Aktualizacja oprogramowania OpenSource skanowania podatności – Greenbone.
2. Zamawiający oświadcza, że posiada stosowne licencje producentów ww. Obszarów Technologicznych, które umożliwiają podniesienie wersji tych Obszarów Technologicznych.
3. Prace związane z podniesieniem wersji oprogramowania, o których mowa w ust. 1, nie mogą być wykonywane w godzinach roboczych u Zamawiającego, jeżeli mogłoby to doprowadzić do sytuacji, w której nie byłoby możliwe korzystanie z danego Obszaru Technologicznego zgodnie z jego przeznaczeniem.
4. Wykonawca powinien dokonać podniesienia wersji oprogramowania, o którym mowa w ust. 1, najpóźniej w terminie 3 miesięcy licząc od chwili otrzymania żądania, o którym mowa w ust. 1.

5. Przed rozpoczęciem prac związanych z podniesieniem wersji Wykonawca powinien poinformować o tym Zamawiającego z wyprzedzeniem co najmniej 5 dni roboczych.
6. Po wykonaniu prac związanych z podniesieniem wersji oprogramowania Wykonawca przeprowadzi konfigurację danego Obszaru Technologicznego, której przeprowadzenie jest niezbędne do prawidłowego funkcjonowania Obszaru Technologicznego zgodnie z jego przeznaczeniem.
7. Zamawiający dopuszcza możliwość wykonywania prac związanych z podniesieniem wersji oprogramowania przy pomocy zdalnego dostępu.

I. Utrzymanie obszarów Technologicznych monitorowania i korelacji zdarzeń bezpieczeństwa rozwiązania SIEM ELK Stack oraz skanowania podatności - Greenbone.

1. Zakres działań:

1) świadczenie usługi monitorowania i korelacji zdarzeń bezpieczeństwa dla urządzeń objętych usługą przy użyciu systemu SIEM (Security Information and Event Management, SIEM, dalej System) oraz systemu skanowania podatności;
2) Monitorowanie systemów w zakresie cyberbezpieczeństwa ma być realizowane w godzinach 8 -17 w dni robocze. Dla godzin nieobjętych monitorowaniem Wykonawca będzie realizował przegląd danych historycznych z okresu nieobjętego stałym monitorowaniem
3) Integracja systemu SIEM z bazami zagrożeń typu threat intelligence: wymagana integracja z bazami Abuse.ch oraz Alienvault OTX
4) Cykliczna aktualizacja sygnatur i reguł działających w systemie SIEM do najnowszych wersji
5) Konfiguracja współpracy systemu SIEM z narzędziami monitorowania ruchu sieciowego typu netflow. W ramach danych analizowanych przez system SIEM ma być dostępna informacja o ruchu sieciowym i wynikających z obserwacji ruchu podejrzanych zdarzeniach takich jak: długo utrzymywane połączenia do sieci zewnętrznych, połączenia o dużym wolumenie ruchu, połączenia typu reverse shell lub tunelowanie, ruch do nieautoryzowanych serwerów smtp, dns, duża ilość pakietów na sekundę, generowana przez pojedyncze urządzenie
6) W zakresie usługi monitorowania będzie zawierało się również konfiguracja systemu SIEM posiadanego przez Zamawiającego. Działanie te ma prowadzić do eliminacji zdarzeń typu false positive czyli stanowiących nieuzasadniony alert generowanych przez system SIEM. Na działanie w tym zakresie wykonawca będzie miał 30 dni od daty podpisania umowy.
7) W ramach działań związanych z monitorowaniem bezpieczeństwa infrastruktury Zamawiający oczekuje przedstawiania comiesięcznych raportów związanych ze zdarzeniami cyberbezpieczeństwa w monitorowanym systemie
8) System SIEM musi zostać skonfigurowany w sposób umożliwiający wykrywanie ataków takich jak:
   - Wykrywanie malware, ransomware, komunikacji typu command and control przy współpracy z zastosowanymi u Zamawiającego systemami AV/EDR;
   - Wykrywanie komunikacji do serwerów klasyfikowanych jako źródła ataków phishingowych;
   - Wykrywanie skanowań wykonywanych w sieci wewnętrznej Zamawiającego, skanowanie portów przy użyciu skanerów typu nmap , nessus, openvas;

- Wykrywanie w sieci Zamawiającego narzędzi i oprogramowania wykorzystywanego do ataków : Kali Linux, Metasploit;
- Wykrywanie ataków na warstwę druga modelu OSI/ISO (typu arp spoofing, mac flooding, ataki na infrastrukturę DHCP, wykrywanie zmian topologii warstwy 2);
- Wykrywanie ataków aplikacyjnych typu cross site scripting, web path traversal, sql injection;
- Wykrywanie ataków na sieć WLAN typu denial of service: deauthentication, podstawienie rogue ap, pojawienie się nowych sieci w pobliżu (przy współpracy z infrastrukturą WLAN Zamawiającego);
- Wykrywanie komunikacji o parametrach odmiennych od standardowych dla danej sieci: tj. ruchu o znaczącym wolumenie, sesji o długim czasie trwania, komunikacji z zasobami na podstawie geolokalizacji odmiennymi od standardowych;
- Wykrywanie działań związanych z zagrożeniami haseł i kont, takich jak: utworzenie nowego administratora, podniesienie uprawnień, użycie konta administratora w godzinach nocnych, ataki typu brute force, konta blokujące się;
- Wykrywanie ruchu do domen typu DGA oraz do domen o niskiej reputacji;
- Monitorowanie spójności i zmian dokonywanych na zasobach takich jak pliki lub klucze rejestru;
- Wykrywanie ataków typu denial of service i distributed denial of service;
- Wykrywanie wycieków danych typu DLP (również użycie urządzeń USB na stacjach roboczych);
- Wykrywanie instalacji nowych urządzeń na stacjach roboczych;
- Wykrywanie użycia zdefiniowanych przez administratora protokołów komunikacyjnych;
- Wykrywanie ruchu administracyjnego (SSH, telnet, RDP) lub ruchu typu VNC, teamviewer (również w zdefiniowanym przez administratora przedziale godzinowym);
- Wykrywanie ruchu typu reverse shell.

9) usługa konfiguracji na infrastrukturze Zamawiającego i integracji Systemu;
10) usługa cyklicznego testowania podatności urządzeń w sieci wewnętrznej;
11) usługa utrzymania i rozwoju Systemu na okres 12 miesięcy;
12) szkolenie w zakresie obsługi dostarczonego Systemu;
13) Usługa utrzymania i rozwoju Systemu ma na celu zapewnienie utrzymania Systemu oraz rozwój sprawności detekcji zdarzeń bezpieczeństwa i optymalizację działania Systemu;
14) przeprowadzenie wstępnego audytu infrastruktury i wykonanie analizy ryzyka dla monitorowanej infrastruktury w terminie 15 dni od daty podpisania umowy;
15) poddanie analizie zapisów ustawy o krajowym systemie cyberbezpieczeństwa pod kątem konieczności zapewnienia zgodności dokumentacji polityki bezpieczeństwa teleinformatycznego MJWPU i spełnienia wymagań wynikających z ww. ustawy w terminie 30 dni od daty podpisania umowy;

2. Główne założenia działania Systemu:

System monitorowania i korelacji zdarzeń bezpieczeństwa (Security Information and Event Management, SIEM) rozumiany jest jako system teleinformatyczny, który gromadzi, parsuje oraz klasyfikuje dane z wielu różnych źródeł a następnie z wykorzystaniem zaawansowanych

mechanizmów analitycznych koreluje zagregowane dane oraz umożliwia detekcję i reagowanie na zagrożenia w czasie rzeczywistym.

3. Szkolenie pracowników w zakresie obsługi posiadanego Systemu obejmie:

1) minimum jednodniowe szkolenie zamknięte przeprowadzone dla 4 osób w języku polskim;
2) szkolenie adresowane dla administratora oraz dla użytkownika Systemu;
3) szkolenie powinno obejmować przynajmniej poziom podstawowy w zakresie administrowania i użytkowania Systemu;
4) szkolenie zawierać będzie zagadnienia teoretyczne oraz praktyczne;
5) szkolenie przeprowadzone w siedzibie klienta lub w przypadku niekorzystnej sytuacji epidemiologicznej przeprowadzone w trybie zdalnym;

4. Świadczenie usług operacyjnych w zakresie:

1) Zarządzanie Systemem na czas trwania Umowy – rekonfiguracje, aktualizacje, rozwiązywanie problemów;
2) Analiza danych agregowanych Systemie i informowanie o zdarzeniach (alertach) i informacjach zdefiniowanych jako istotne poprzez przesłanie wiadomości na wskazane przez Zamawiającego adresy email, w całym okresie współpracy; czas reakcji i informowania o problemie nie przekroczy 4 godzin roboczych w przypadku zdarzeń o wysokim i krytycznym priorytecie;
3) Przeprowadzanie skanowania podatności urządzeń w sieci wewnętrznej w cyklach trzymiesięcznych. Każdorazowo przygotowany zostanie raport zawierający listę znalezionych podatności oraz rekomendacje dotyczące ich usunięcia lub mitygacji;
4) Przygotowanie i przesyłanie comiesięcznych raportów podsumowujących działanie Systemu, wykryte problemy oraz podatności.